

Department of Justice

§ 17.80

keep a record of the vaults and security containers under their cognizance along with the designation of the level of classified information authorized to be stored therein.

§ 17.76 Changing combinations to security containers.

Combinations to security containers and dial-type locks will be changed only by individuals having an appropriate security clearance and who have received instruction on how to correctly change such combinations. Combinations shall be changed:

- (a) When the container is placed in use;
- (b) When an individual knowing the combination no longer requires or is authorized access to classified information stored in the container;
- (c) When the combination or record of combination has been subject to compromise;
- (d) When taken out of service; or
- (e) At least annually.

§ 17.77 Equipment out of service.

When security storage equipment is taken out of service, it shall be inspected to ensure that no classified information remains.

(a) Security Programs Managers shall establish procedures to certify that whenever security equipment is moved or relocated or "out of service" or "excess" that the security equipment does not contain classified information.

(b) When taken out of service, built-in combination locks shall be reset to the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30.

§ 17.78 Classification of combinations.

The combination of a vault or container used for the storage of classified information and material shall be assigned a security classification no lower than the highest level of the classified material authorized to be stored therein. No downgrading/declassification instructions or classifier identity are required to be made when classifying records of combinations to security containers. Accordingly, classification actions for such combinations are not required to be reported.

Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes.

§ 17.79 Recording storage facility data.

A record shall be maintained by Security Programs Managers or their designees for each vault, secure area, or container used for the storage of classified information. The record shall show its location, and the names and other appropriate identifying data of persons having knowledge of the combinations to such storage facilities. General Services Administration Optional Form 63, entitled, "Security Container Information" may be used within the Department for these purposes. The OF-63 containing security combinations shall be marked with the appropriate overall classification, and shall be safeguarded and stored in accordance with the protection afforded to that classification.

§ 17.80 Care during working hours.

Each individual shall take all necessary precautions to prevent access to classified information by unauthorized persons (i.e., persons who do not possess an appropriate security clearance, and who do not possess the required need-to-know). Among the precautions to be followed are:

(a) Classified documents, when removed from storage for working purposes, shall be kept under constant surveillance and turned face-down or covered when not in use. Department Cover Sheets should be utilized to cover classified documents.

(b) Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information shall be either destroyed by the person responsible for their preparation immediately after they have served their purposes, or shall be given the same classification and safeguarded in the same manner as the classified information they contain.

(c) Classified information handled by word processors or remote terminals is susceptible to interception by unauthorized persons due to unintended electrical emanations. Word processors or remote terminals used frequently to handle classified information must